Claims 1-5, 7-11, 20-29, 41-42, 49-53, 55-67 and 76-79 are cancelled.

Claims 6, 12-19, 30-40, 43-48, 54 and 68-75 were cancelled previously.

New claims 80-100 are added as follows:

1-79 (Cancelled).

80. (New) A method comprising:

receiving a request to transfer application data from a source computing device to a destination computing device; and

determining if the requested application data is unconditionally non-migrateable to another computing device and not transferring the requested application data in response to that determination.

81. (New) A method as recited in claim 80, and further comprising determining if the requested application data is user-migrateable and in response thereto:

receiving input identifying a user-defined passphrase;

identifying an encryption key previously used to encrypt the application data,

encrypting the encryption key based at least in part on the user-defined passphrase, and

transferring the encrypted encryption key to be copied to the destination computing device.

82. **(New)** A method as recited in claim 81, and further comprising transferring the encrypted application data to the destination computing device.

83. **(New)** A method as recited in claim 80, further comprising:

receiving other application data to be stored on the source computing device;

determining if the other application data is non-migrateable and in response to that determination:

encrypting the other application data using a non-migrateable encryption key; and

storing the encrypted other application data on the source computing device.

84. **(New)** A method as recited in claim 83, further comprising:

receiving a request to transfer the other application data from the source computing device to a destination computing device; and

determining that the other application data is non-migrateable and not transferring the other application data in response to that determination.

85. **(New)** A method as recited in claim 83, further comprising:

determining if the other application data is user-migrateable in accordance with a user-defined passphrase and in response to that determination:

encrypting the other application data using an other encryption key; and

storing the encrypted other application data on the source computing device.

86. **(New)** A method as recited in claim 85, further comprising:

receiving a request to transfer the other application data from the source computing device to a destination computing device, the request including the user-defined passphrase;

encrypting the other encryption key using the user-defined passphrase, and

transferring the encrypted other encryption key to the destination computing device.

87. **(New)** A method as recited in claim 86, and further comprising transferring the encrypted other application data to the destination computing device.

88. **(New)** One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a source computing device, causes the one or more processors to:

receive a request to transfer application data from a source computing device to a destination computing device; and

determine if the requested application data is unconditionally non-migrateable to another computing device and not transfer the requested application data in response to that determination.

89. **(New)** One or more computer readable media as recited in claim 88, wherein the plurality of instructions further causes the one or more processors to:

receive input identifying a user-defined passphrase;

identify an encryption key previously used to encrypt the application data,

encrypt the encryption key based at least in part on the user-defined passphrase, and

transfer the encrypted encryption key to be copied to the destination computing device.

90. **(New)** One or more computer readable media as recited in claim 89, wherein the plurality of instructions further causes the one or more processors to transfer the encrypted application data to the destination computing device.

91. **(New)** One or more computer readable media as recited in claim 88, wherein the plurality of instructions further causes the one or more processors to:

receive other application data to be stored on the source computing device; and

determine if the other application data is non-migrateable and in response to that determination:

encrypt the other application data using a non-migrateable encryption key; and

store the encrypted other application data on the source computing device.

92. **(New)** One or more computer readable media as recited in claim 91, wherein the plurality of instructions further causes the one or more processors to:

receive a request to transfer the other application data from the source computing device to a destination computing device; and

determine that the requested other application data is non-migrateable and not transfer the requested application data in response to that determination.

93. **(New)** One or more computer readable media as recited in claim 91, wherein the plurality of instructions further causes the one or more processors to:

determine if the other application data is user-migrateable in accordance with a user-defined passphrase and in response to that determination;

encrypt the other application data using an other encryption key; and

store the encrypted other application data on the source computing device.

94. **(New)** One or more computer readable media as recited in claim 93, wherein the plurality of instructions further causes the one or more processors to:

receive a request to transfer the other application data from the source computing device to a destination computing device, the request including the user-defined passphrase;

encrypt the other encryption key using the user-defined passphrase, and

transfer the encrypted other encryption key to the destination computing device.

95. **(New)** One or more computer readable media as recited in claim 94, wherein the plurality of instructions further causes the one or more processors to transfer the encrypted other application data to the destination computing device.

96. **(New)** A computer-implemented method comprising:

receiving a request to transfer encrypted data from a source computing device to a destination computing device;

checking whether the encrypted data can be transferred to the destination computing device in accordance with a user-defined passphrase;

querying a user for the user-defined passphrase;

encrypting an encryption key based at least in part on the user-defined passphrase; and

transferring the encrypted encryption key to the destination computing device.

97. **(New)** The computer-implemented method of claim 96, further comprising:

transferring the encrypted data to the destination computing device;

decrypting the encrypted encryption key at the destination computing device using the user-defined passphrase; and

accessing the encrypted data at the destination computing device by way of the decrypted encryption key.

98. **(New)** A computer-implemented method comprising:

receiving a request to transfer application data from a source computing device to a destination computing device;

determining that the requested application data is unconditionally non-migrateable to another computing device, the determination based at least in part on a non-migrateable encryption key stored on the source computing device; and

not transferring the requested application data to the destination computing device in response to the determination.

99. **(New)** One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a source computing device, causes the one or more processors to:

receive a request to transfer encrypted data from a source computing device to a destination computing device;

check whether the encrypted data can be transferred to the destination computing device in accordance with a user-defined passphrase;

query a user for the user-defined passphrase;

encrypt an encryption key based at least in part on the user-defined passphrase; and

transfer the encrypted encryption key to the destination computing device.

100. (New) One or more computer readable media as recited in claim 99, wherein the plurality of instructions further causes the one or more processors to transfer the encrypted data to the destination computing device.